INTEGRATED IDENTITY MECHANISM FOR UBIQUITOUS SERVICE ACCESS

Mohammad M. R. Chowdhury
UniK – University Graduate Center
P.O. Box 70, N-2007 Kjeller, Norway.
mohammad@unik.no

Josef Noll
UniK – University Graduate Center
P.O. Box 70, N-2007 Kjeller, Norway.
Josef@unik.no

ABSTRACT

Ubiquitous access and pervasive computing enable innovative services and provide the service access in every situation. People currently rely on numerous forms of identities to access the remote or proximity services. The inconvenience of possessing and using these identities creates significant security vulnerability. This paper proposes an architecture that integrates the identities required to access various remote and proximity services into a single mechanism. In the mechanism, identities are distributed between the user's personal device and a secure network space. Third party identity providers along with the mobile network provide the underlying secure infrastructure for identity information exchange. The use of multiple layers of authentication context to meet several levels of secure service access requirements enhances the security of this mechanism.

KEYWORDS

Identity management, remote service, proximity service, security.

1. INTRODUCTION

Now-a-days, fixed and fixed wireless broadband networks are not the only means to access diverse web services. Ubiquitous access and pervasive computing enable the service access in every situation. Mobile network can provide sufficient capacity for real time data communication. The deployment of state-of-the-art technology in core networks is allowing fixed and mobile services to be seamlessly mixed. In addition to the remote (web) services, introduction of near field communication (NFC) at usage in mobile phones can enable many new proximity services [1]. All these significant developments in network capabilities and service world diversifications can boost innovative service interaction.

User identity handling will play a vital role for accessing diverse services. Now-a-days, service access in Internet is burdened with many user names and passwords. Reuse of these is frequent and unsafe. Service providers also use substantial efforts managing and assigning identities to the users. Gartner predicted in its annual IT security summit 2005, 80% of organizations will reach a password breaking point by 2007 [2]. Numerous Physical identities are used to identify its owner to various services. Recently, people increasingly use smart cards for service access with electronic chip and memory embedded in these. It enhances the security and allows storage of user details on the card. To meet additional security requirements, the possession factor of physical/online identities is often enhanced by a knowledge factor, a PIN code. If there are several of these, users tend to compromise security by writing their PIN codes. It is evident that the current forms of identities are inconvenient to use and manage both for the users and service providers. Therefore, the service access scenarios ask for a new form of identity management.

That is why an integrated identity mechanism is suggested in this paper to overcome these deficiencies of current identities. The proposed solution is expected to integrate the identities required to access both the remote and proximity services into a single mechanism. The identities are distributed between the user's personal device and a secure network space. Third party identity providers along with the mobile networks provide the underlying security infrastructure for identity information exchange. The proposed mechanism has the potential to eliminate not only the numerous usernames and passwords but also the use of various physical identities. In addition to user's convenience, such identity mechanism might also be useful for other stakeholders like, identity providers, service/application providers, and equipment vendors.

The section 2 presents the related work in this area. The following section illustrates the nature of ubiquitous services. The proposed identity mechanism and the service access demonstration based on the mechanism are discussed in section 4 and 5. Section 6 states the benefits of the stakeholders involved in the proposed identity mechanism and the paper concludes with section 7.

2. RELATED WORK

Managing identities is crucial for the development of the next generation of distributed applications and services. Ubiquitous access, sufficient bandwidth by mobile networks and capabilities of SIM can bring in many new services in mobile environments. Identity management should also consider utilizing the strengths of the mobile environments. Numerous research works are going on in various institutes and industries to provide better identity management solutions. In one approach, J. Altman and R. Sampath proposed a user-centric network identity management framework in [3]. The paper suggested a unifying identity solution to integrate the multiple user credentials currently stored by service providers independently. The authors only concentrated on the identity management issues over the Internet. In another solution [4], the authors presented a framework for identity management in a distributed environment. The solution was proposed to support secure and convenient access to web-based applications and services. Most of the present research works are concentrating on managing user identities over the Internet [5], [6], [7], [8]. However, some of the initiatives also consider the capabilities and challenges of mobile environment in identity management [9], [10], [11]. It is to be noted that user identities include not only the username/password/PIN codes for accessing remote service but also many physical identities to access many proximity services. All these efforts lack solutions for handling the physical identities.

There are significant initiatives from ICT industries to provide real life solutions in this area. In Liberty Alliance [12], members are working to build open standard-based specifications for federated identity and interoperability in multiple federations, thereby foster the usage of identity-based web services. Within this, they are focusing on end user privacy and confidentiality issues and solutions against identity theft. Another solution, Sxip [13] has been designed to address the Internet-scalable and user-centric identity architecture. It provides user identifications, authentications and internet form fill solutions using web interfaces for storing user identity, attribute profiles and facilitating automatic exchange of identity data over the Internet. To access online services, Windows CardSpace [14] uses various virtual cards (mimic physical cards) issued by the identity providers for user identifications and authentications, each retrieving identity data from an identity provider in a secure manner. Banking industry of Norway with a partnership of a mobile operator initiated BankID [15] for identification and signing agreement on the move. BankID for mobile phones will initially be used in four areas: logging on to Internet banks, mobile banking, electronic service for business and the public sector, and account-based payment service for internet and mobiles. Gemalto [16] provides online and offline identity management and security solutions in the form of various smart cards with associated software, middleware and server-based solutions. NXP [17] is also offering identification products in areas like government, banking, access control etc. using secure innovative contactless smart cards and chips. MasterCard is currently running a trial in Dallas, Texas for touch and go payment via NFC-enabled mobile phone with MasterCard PayPass capability [18]. The main focus of these is towards the identity management in Internet domain (remote services), but some of the solutions also target services located in the proximity of users. For ubiquitous service access, the big challenge will be to integrate these scattered user's identities into a single mechanism. The proposed integrated identity management mechanism is expected to address this challenge. The mechanism engages the SIM card as storage place for identities and uses the mobile network as secure underlying infrastructure.

3. UBIQUITOUS SERVICE WORLD

Now-a-days people can access services from anywhere and any time, whenever it is necessary. Ubiquitous access and pervasive computing make these possible. The section will address the nature of the two types of services, remote services and proximity services.

3.1 Remote services

The introduction of state-of-the-art ubiquitous networks offers sufficient capacity, QoS and interoperability and allows the users to interact with numerous services remotely. Social communications (exchanging messages, voice, photos, videos), online shopping, reservation and banking, remote home or office network access are few examples of remote services. Fixed-mobile convergence [19] and thereby seamless user experience can boost such service creations and intake by users. These services are currently accessed through the Internet using different authentication mechanisms. This form of identification and authentication can be termed as *'something you know'* (knowledge based) and sometimes *'something you have'* (possession based) [20]. Users have to register prior to first usage and publish private information, often more than what is strictly necessary for service access. The access is often granted through username/ password/ PIN. Having usernames/passwords is an example of *some you know* and possessing a smart card to generate one-time-password (OTP) is an instance of *something you have*.

3.2 Proximity services

The second group of services happens in the proximity of the users at local access points. These services are accessed through physical interactions with physical cards or devices, e.g. payment cards and admittance cards. This form of identification can be said as *'something you have'*. Depending on the security requirements of the services, the possession based authentication might be enhanced by a knowledge factor (e.g. PIN code) add on. The devices/ cards and PIN codes are issued to the users when registered for relevant services. The introduction of near field communication (NFC) technology makes the transfer of user's information from one device to another possible. This will obviously boost the intake of proximity services.

In the ubiquitous service world, the border between remote services and proximity services is not strict. Proximity services like NFC may initiate remote services like ticket ordering for cinema tickets [1]. The next section discusses the detail of proposed integrated identity mechanism.

4. INTEGRATED IDENTITY MECHANISM

The ubiquitous service world and deficiencies of current form of identities demand an integrated mechanism of managing user's identities. The proposed integrated identity mechanism consists of certificates, keys and preferences stored in a personal device and in the network. These identities are categorized broadly into personal identity (PID), corporate identity (CID) and social identity (SID) based on the roles exercised by a person in real life [21]. PID can be used to identify ourselves in our very personal and commercial interactions. CID and SID can be used in our professional and social interactions respectively.

4.1 The role of identity provider

State/government is the traditional and most accepted identity provider in national and international level. With strong regulations in place, banks and mobile operators can also act as an identity provider (IDP). User separately makes an agreement with the IDP for the identity services. The role of an IDP is strictly regulated. It is maintaining a strong trust relationship between the subscribers and other IDPs. It makes use of the mobile network along with phone and SIM card as the secure infrastructure for storing and exchanging identity information in the proposed solutions. If PC is used for user identity based service interaction, mobile network has the potential to be the return channel for authentication purpose. There are reasons why

we think the existing mobile network infrastructure is ideal for identity services like user authentication and consent such as,

- Mobile network's global acceptability, interoperability and reach.
- The security of 3G mobile systems has been strengthened by introducing longer cipher key, mutual (network, user) authentication, signaling and data traffic integrity and extension of ciphering back into the network [22].
- In addition to Bluetooth and Infrared, introduction of NFC makes the proximity service more accessible.

Introduction of mobile communication technology as a mean to provide identity service also brings new challenges, for example,

- Minimizing the consequences of mobile terminal's loss or theft.
- Restoration of user's ongoing session, dropped due to poor and erratic RF signal quality.
- Handling and user interface, especially referring to complex transactions.
- Emerging number-portability legislation is making interoperability even more complicated and more critical.

4.2 The concepts and elements

In the proposed mechanism, mobile network together with mobile phone provides the underlying infrastructure. A trusted and well-accepted third party can play the very important identity provider's role. In addition to subscription for voice and data service, user will also need to subscribe for identity services to IDP. It then issues a certificate to the user and allocates a secure identity space in the network. User identity data and attributes are distributed and stored into two places. A part of the user identities that contain very sensitive user information like, $PID_{Bank/Creditcard}$, $PID_{Home\ admittance}$ will be stored (permanently or temporarily) in the SIM card of mobile phone. Therefore, these are having very strict authentication requirements. SIM card is considered as storage place because it can be revoked, user now-a-days can rarely be found without a mobile phone and there are possibilities of further security enhancements. For example, BankID partnership [15] will provide user a public key infrastructure (PKI) built in SIM card for identification and signing the agreement. Another part of user identities which need low authentication requirements, for example social identities and preferences (SID), will be stored into the secure identity space in the network. To manage multiple credentials, a trusted third party/service provider can load additional IDs confidentially to either at SIM card or at network identity space with user's consent so IDP/operators do not see the data being loaded. In case of loosing SIM card, new one can be ordered and the identities previously stored in the card can be reloaded.

With the identity subscription certificate user can authenticate himself to access the network identity repository that contains identities for example SIDs. These identities will be used to access services that need medium or low level of security requirements. There can be many social identities of a user. SIM card holds only the most sensitive user identities. Therefore, a space in the network is considered which may not be so secure but secure enough for storing these less sensitive identities. To make the remote service access hassle-free, the concept of Circle of Trust (COT) developed by Liberty Alliance can be employed [2]. For remote service access, user can have single sign-on (SSO) functionality to move seamlessly between federated service/content/identity providers using a single SIM card credential (or identity subscription certificate) without entering numerous usernames and passwords. The identity subscription certificate issued by an IDP is not enough to access services that need additional security requirements. PIDs/CIDs stored in the SIM card have to be used to meet such requirements. Besides the mobile environment, services can also be accessed from PC when identity subscription certificate (issued by IDP) and user's PID/CID/SIDs are available from PC.

Introduction of near field communication (NFC) technology adds intelligence and networking capabilities to the phone and creates many new opportunities to add product and service capabilities to handset like digital transactions in very good proximities. It can make a mobile phone an ideal device for payments and gaining access [23], [24]. Less sensitive admittance keys can be stored at network identity space and when required can be downloaded temporarily to the SIM card memory. To access proximity services, the identity information stored in SIM card (permanently or temporarily) can be transmitted through the NFC interface. The channel between two NFC devices can be secured using available cryptographic protocols [25].

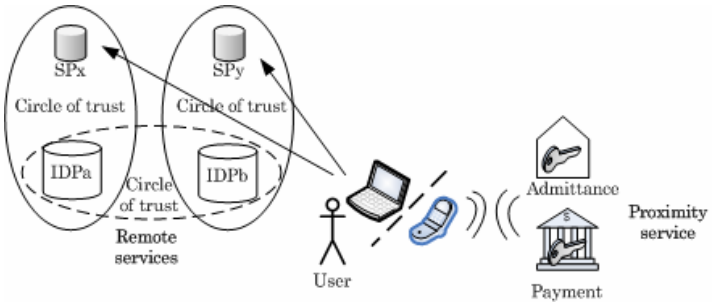

Figure 1 A generic diagram for integrated identity mechanism and service access.

Figure 1 shows a generic conceptual diagram for the proposed integrated identity mechanism where both remote and proximity service access scenarios have been considered.

4.3 Authentication mechanisms

Different levels of authentication mechanisms need to be maintained depending on service access security requirements. From user point of view, a strictly maintained secure environment/channel is required to exchange very sensitive user information with the service provider. Some of the service access scenarios need minimum user information exchange. These may not require highly secured infrastructure. Besides from service provider's point of view, building or maintaining very strict secure channel requires good investment as well. Therefore, different levels of security should be employed for different types of services. Analyzing all these aspects, [23] introduced three levels of security: *Nice to know*, *need to know*, *have to know* (see figure 2).

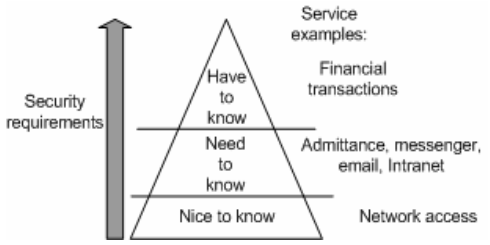

Figure 2 Security infrastructure based on security requirements.

Nice to know services are for example, network access, where knowledge about usage is only required. *Need to know* services like Intranet or VPN access, admittance have higher security requirements. Highest security requirements have to be met for *have to know* services, such as credit card or bank transactions.

Table 1 Identity types, realizations, storage, and security requirements.

Identity	Examples	Realization	Location	Security requirement
PID	$PID_{Bank/Creditcard}$	Certificate + (private + public) key	SIM	High
	$PID_{Home\ admittance}$	Home entry key		
CID	$CID_{Office\ admittance}$	Office entry key	SIM	High
	$CID_{other\ admittance}$	Temp. entry keys	Network	Medium
SID	Preferences	foaf	Network	Low
	Attributes	foaf		Medium

Table 1 gives several examples of PIDs, CIDs and SIDs, their possible realizations and where these identities will be located or stored. Considering the various levels of security, the corresponding security requirement of each identity is also mentioned. As the SIM contains the identities with highest security requirements and also entitles the owner access to his/her network identity space, an extra protective measure should be employed for accessing SIM to make PIDs more secure. To address this, an extended SIM (ESIM)

is proposed which is a customized SIM card. It has two modules: one is responsible for operator service access and access to network identity space containing SIDs. The other part contains the highly sensitive personal identities with protection through additional PIN code. Therefore, the solution has several layers of security provisions. *Something you have* which is a smart card (ESIM) gives low level of security, and *something you know*, a knowledge based ones (PIN codes) provide medium or high level of security.

5. SERVICE ACCESS DEMOSTRATION

In this section, two service access architectures have been illustrated in Figure 3 and 4 based on the proposed integrated identity mechanism. In the first figure user requesting a service that needs low level security requirement. Figure 4 shows the steps for the service access that need higher level of security.

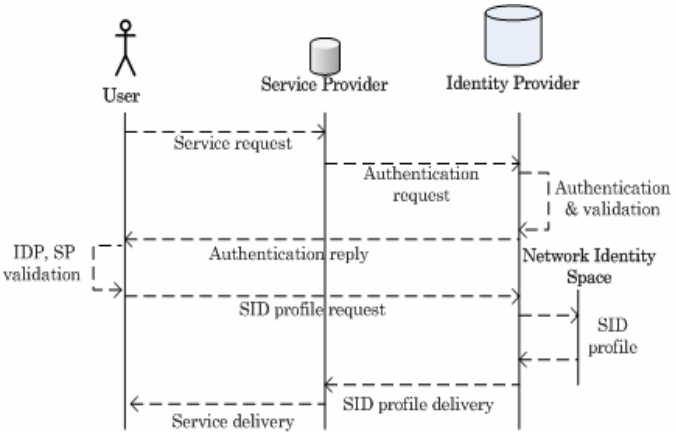

Figure 3 User requests a service that requires user's SID profile.

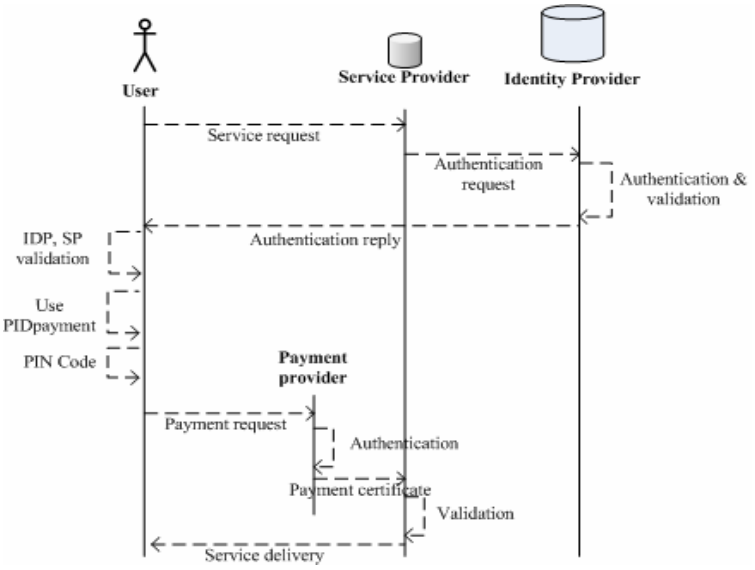

Figure 4 User requests a service that requires $PID_{payment}$.

Use sends a message to service provider requesting for a service. The message contains the user certificate provided by the IDP during identity subscription. Service provider (SP) then forwards this certificate with its own one and asks the IDP for authenticating the user. IDP authenticates the user and SP and returns a reply. All these message exchange happens in a secure manner using strong encryption mechanism. User checks the validity of the reply and requests IDP to deliver his/her SID profile (stored in

secure identity space) to SP. Figure 4 shows a service request (payment) that needs to meet a high level of security requirement. Therefore, after checking the validity of the authentication reply, user applies his/her $PID_{payment}$ for payment of the service using a *'something you know'* authentication mechanism, a PIN code. Payment provider forwards the payment certificate to SP and after checking its validity service is delivered. These service demonstrations depict the use of proposed integrated identity mechanism for accessing various types of services in a secure manner.

6. STAKEHOLDER'S BENEFITS

Users, identity providers, service/application providers and equipment vendors every associated entity can be benefited through the proposed integrated identity mechanism.

User is benefited through easy-to-use and mobility in service interactions at a lower cost. With strong security mechanism in place by the underlying infrastructure, the proposed identity mechanism can ensure more secure service access. Single sign-on (SSO) through use of COT allows users to move seamlessly without entering numerous user names and passwords [12]. Use of NFC makes this identity mechanism more accessible to innovative proximity services. Finally, hassle-free service access is a main feature of this mechanism.

Revenues can be generated through providing identity services including user authentication and consent, and infrastructure sharing, including SIM, with other identity providers (when operators choose not to be the identity providers because of trust). Mobile/wireless operators can extract value from their infrastructure investment with the increase in data traffic over their licensed airwaves and expansion of their brand's reach. The identity service provision positions the mobile network as a preferred channel for trusted services.

Service provider benefits generally derive from a lower cost-of-business and more service intake by users. User is motivated to use more services as integrated identity mechanism provides, hassle-free usage, security, ease of use and availability. Use of identity provider services for user's authentication lowers the cost of business (by not maintaining an individual authentication mechanism), integration efforts and accelerates time-to-market.

Mobile vendors, including network infrastructure, devices and platform, and smart card/chip vendors benefit from an increased demand for standardized, higher-end devices and interfaces. User demand for identity-enabled services accelerates device renewal. Higher demand leads to volume savings in production cost. Multi-functional and easy to use terminals increase user experience and brand loyalty.

7. CONCLUSION

The paper introduces an integrated mechanism for identity provision that facilitates both remote service and proximity service access. It addresses the concerns that user can longer cope with the current identity usage scenarios. The proposed mechanism suggests the storage of user identities in a distributed manner. A customized SIM card is proposed that stores most sensitive user identities. Less sensitive ones are stored at a secure user identity space in the network. Multiple factors of authentication mechanisms are employed to address different levels of security requirements. The paper also demonstrates service access architectures using the proposed identity mechanism. The use of such an integrated identity concept can benefit the application/service industries, infrastructure vendors and above all, the users. In our future work, we will focus on implementing a use case and prototype on seamless user experience in heterogeneous wireless networks.

ACKNOWLEDGEMENT

The contribution is a part of an ongoing research in WP2 of SWACOM project, funded by The Research Council of Norway. The authors would like to acknowledge the contributions and supports provided by their colleagues from UniK, Kjeller and Telenor R&I, Fornebu, Norway.

REFERENCES

[1] NFC forum, http://www.nfc-forum.org/

[2] Mohammad M R Chowdhury, J.Noll, 2007, Distributed Identity for Secure Service Interaction, P*roceedings of the Third International Conference on Wireless and Mobile Communications, ICWMC07*, Gaudeloupe, French Caribbean.

[3] Altmann, J., Sampath, R., 2006, UNIQuE: A User-Centric Framework for Network Identity Management, *Network Operations and Management Symposium, NOMS 2006*, Vancouver, Canada, pp. 495-506.

[4] Jingsha He, Ran Zhang, 2005, Towards Formal Framework for Distributed Identity Management, *Web Technologies Research and Development – APWeb 2005*, Springer Berlin / Heidelberg, pp. 913-924.

[5] Buell, D. amd Samdhu, R., 2003, Identity Management, *IEEE Internet Computing*, Vol. 7, No. 6, pp. 26-28.

[6] Dongwan Shin, Gail-Joon Ahn, and Prasad Shenoy, 2004, Information Assurance in Federated Identity Management: Experimentations and Issues, *Web Information Systems – WISE 2004*, Springer Berlin / Heidelberg, pp. 78-89.

[7] Oliver Berthold and Marit Köhntopp, 2001, Identity Management Based on P3P, *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability*, Springer Berlin / Heidelberg, pp. 141-160.

[8] Vassilis Poursalidis and Christos Nikolaou, 2006, A New User-Centric Identity Management Infrastructure for Federated Systems, *Trust and Privacy in Digital Business*, Springer Berlin / Heidelberg, pp. 11-20.

[9] Siddiqi, J. et al., 2006, Secure ICT Services for Mobile and Wireless Communications: A Federated Global Identity Management Framework, *Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06)*, Nevada, USA, pp. 351-357.

[10] Mario Hoffmann, 2004, User-centric Identity Management in Open Mobile Environments, *Privacy, Security and Trust within the Context of Pervasive Computing*, Springer Netherlands, pp. 99-104.

[11] Audun Jøsang, Mohammed AlZomai, Suriadi Suriadi, 2007, Usability and Privacy in Identity Management Architectures, *Proceedings of the Australian Information Security Workshop (AISW'07)*, Victoria, Australia.

[12] Liberty Alliance Project, http://www.projectliberty.org/

[13] Sxip Identity, http://www.sxip.org/

[14] Windows CardSpace, http://cardspace.netfx3.com/

[15] BankID: Delivering Bank-common Trust for Web-based Transactions, https://www.cybertrust.com/intelligence/case_studies/ [Retrieved on April 2, 2007]

[16] Gemalto, http://www.gemalto.com/

[17] NXP Semiconductors, http://www.nxp.com/

[18] Cellular-news, "MasterCard Tests NFC Payments with Nokia Handsets", http://www.cellular-news.com/story/20211.php [Retrieved on April 2, 2007]

[19] Fixed-Mobile Convergence Alliance, http://www.thefmca.com/

[20] Two-factor authentication, http://en.wikipedia.org/wiki/Strong_authentication

[21] Mohammad M. R. Chowdhury, J. Noll, 2006, Service Interaction through Role based Identity, *Proceedings of Wireless World Research Forum Meeting 17*, Heidelberg, Germany.

[22] K. Boman, G. Horn, P. Howard and V. Niemi, 2002, UMTS security, *Electronics and Communication Engineering Journal*, Volume 14, Issue 5, pp. 191-204.

[23] J. Noll, J.C. Lopez Calvet, K. Myksvoll, 2006, Admittance services through mobile phone short messages, *Proceedings of the International Conference on Wireless and Mobile Communications ICWMC'06*, Bucharest, Romania.

[24] J. Noll, U. Carlsen, G. Kalman, 2006, License transfer mechanisms through seamless SIM authentication, *International Conference on Wireless Information Systems, Winsys 2006*, Setubal, Portugal.

[25] Haselsteiner, Ernst and Breitfuss, Klemens, 2006, Security in Near Field Communication (NFC) Strengths and Weaknesses, *Workshop on RFID Security - RFIDSec 06*, Graz, Austria.